OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

August 6, 2002

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
CHIEF INFORMATION OFFICER OF THE JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER

SUBJECT: National Information Assurance Acquisition Policy

References: (a) Department of Defense (DoD) Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) 6-8510 "Global Information Grid Information Assurance", dated June 16, 2000,
(b) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Information Assurance Acquisition Policy

Reference (a) issued policy and guidance on securing and assuring the Global Information Grid (GIG). It specifies a defense-in-depth strategy for applying integrated layered protection to GIG information systems and networks through a combination of properly trained people, IA operations, and sufficiently robust and well understood technology. Reference (a) also specifically directed DoD compliance with reference (b), the relevant parts of which are quoted in the attachment.

The purpose of this memorandum is to restate and emphasize that DoD must continue to comply with the spirit and intent of reference (b). Therefore, all IA products,[1] and IA-enabled IT products[2] that require use of the product's IA capabilities, acquired under contracts executed after July 1, 2002 to support all DoD information systems must be evaluated and validated, but with the following necessary qualifications.

[1] IA Product. An IT product or technology whose primary purpose is to provide confidentiality, authentication, integrity, access control and non-repudiation of data; correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls and intrusion detection devices.

[2] IA-Enabled Product. A product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples of IA-enabled products include security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems. If there is no requirement to use (enable) the IA capabilities of these products in the application for which they are acquired, then the products do not have to be evaluated.

a. If an approved U.S. Government protection profile exists for a particular product type and there are validated products available for use, then acquisition is restricted to those products or to products that vendors, as a condition of purchase, submit for evaluation and validation to the approved protection profile.

b. If an approved U.S. Government protection profile exists for a particular product type and no validated products are available for use, the acquiring organization must require, as part of the selection process, that vendors submit their products for evaluation and validation to the approved protection profile.

c. If no U.S. Government protection profile exists for a particular product type, the acquiring organization must require, as part of the selection process, that vendors provide a security target that describes the security attributes of their products, and that the vendors submit their products for evaluation by a NIAP certified laboratory at a minimum of EAL 2.

d. Contracts shall specify that product validation will be kept current through vendors submitting the next version of their products for evaluation or through participation in the NIAP Assurance Maintenance Program, which only requires validation of changes to products. All NSA/NIST protection profiles will require participation in the assurance maintenance program.

e. Products that are available under multiple-award schedule contracts or non-DoD Government-Wide Acquisition Contracts[3] awarded before July 1, 2002 must be evaluated when and if an updated version of the product is made available under the contract.

f. Although products pending evaluation may be used, contracts shall require that any evaluations initiated under the conditions described in sub-paragraphs b. through e. above, must be satisfactorily completed within a specified period of time.

g. Implementation of security related software patches directed through the DoD Information Assurance Vulnerability Alert Program shall not be delayed pending NIAP evaluation of changes that may result from the patches.

[3] For example, GSA schedules and other contract vehicles established by other federal departments or agencies that are available for DoD use.

A significant feature of this guidance is that it virtually eliminates the need for waivers to the provisions of NSTISSP No. 11. It will also be incorporated into a new DoD instruction on IA implementation that has already been formally coordinated within DoD and will be issued soon. Further, the DoD IG's office has indicated that implementation of this policy will be subject to review during FY 2003, so it is important that the guidance be widely disseminated as soon as possible. Please direct any questions to Mr. Eustace King in the Defense-wide Information Assurance Program (DIAP) office. He can be reached at (703) 602-9969 or e-mail: eustace.king@osd.mil.

Priscilla Guthrie
Deputy Chief Information Officer

Enclosure: AS

## Excerpt from the National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled IT Products

## SECTION I - POLICY

1. Information Assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition appropriate implementation of evaluated or validated Government Off-the Shelf {GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products*. These products should provide for the availability the systems, ensure the integrity and confidentiality of information, and the authentication and non-repudiation of parties in electronic transactions.

2. Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

a. The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

b. The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

c. The NIST Federal Information Processing Standard (FIPS) validation program.

The evaluation/validation of COTS IA and IA-enabled IT products will be conducted by accredited commercial laboratories, or the NIST.

3. By 1 July 2002, the acquisition of all COTS IA and IA-enabled products to be used on the systems specified in paragraph 2., above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in subparagraphs 2.a. through 2.c.

4. The acquisition of all GOTS IA and IA-enabled products to be used on systems entering, processing, storing, displaying, or transmitting national security information shall be limited to products which have been evaluated by the NSA, or in accordance with NSA-approved processes.

5. Normally, a complementary combination of IA/IA-enabled products is needed to provide a complete security solution to a given environment. Thus, in addition to employing evaluated and validated IA/IA-enabled products, a solution security analysis

should be conducted as part of the certification and accreditation process. In support of this, NSA shall provide guidance regarding the appropriate combinations and implementation of GOTS and COTS IA and IA-enabled products.

6. Subject to policy and guidance for non-national security systems, departments and agencies may wish to consider the acquisition and appropriate implementation of evaluated and validated COTS IA and IA-enabled IT products. The use of these products may be appropriate for systems which process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures as defined in Presidential Decision Directive No. 63 {PDD-63), Critical Infrastructures Protection.

## SECTION II - RESPONSIBILITIES

7. Heads of U.S. Departments and Agencies are responsible for ensuring compliance with the requirements of this policy.

## SECTION III - EXEMPTIONS AND WAIVERS

8. COTS or GOTS IA and IA-enabled IT products acquired prior to the effective dates prescribed herein shall be exempt from the requirements of this policy. Information systems in which those products are integrated should be operated with care and discretion and evaluated/validated IA products and solutions considered as replacement upgrades at the earliest opportunity.

9. Waivers to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for waivers, including a justification and explanatory details, shall be forwarded through the DIRNSA, ATTN: V1, who shall provide appropriate recommendations for NSTISSC consideration. Where time and circumstances may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is authorized to approve waivers to this policy which may be necessary, to support U.S. Government operations which are time-sensitive, or where U.S. lives may be at risk.